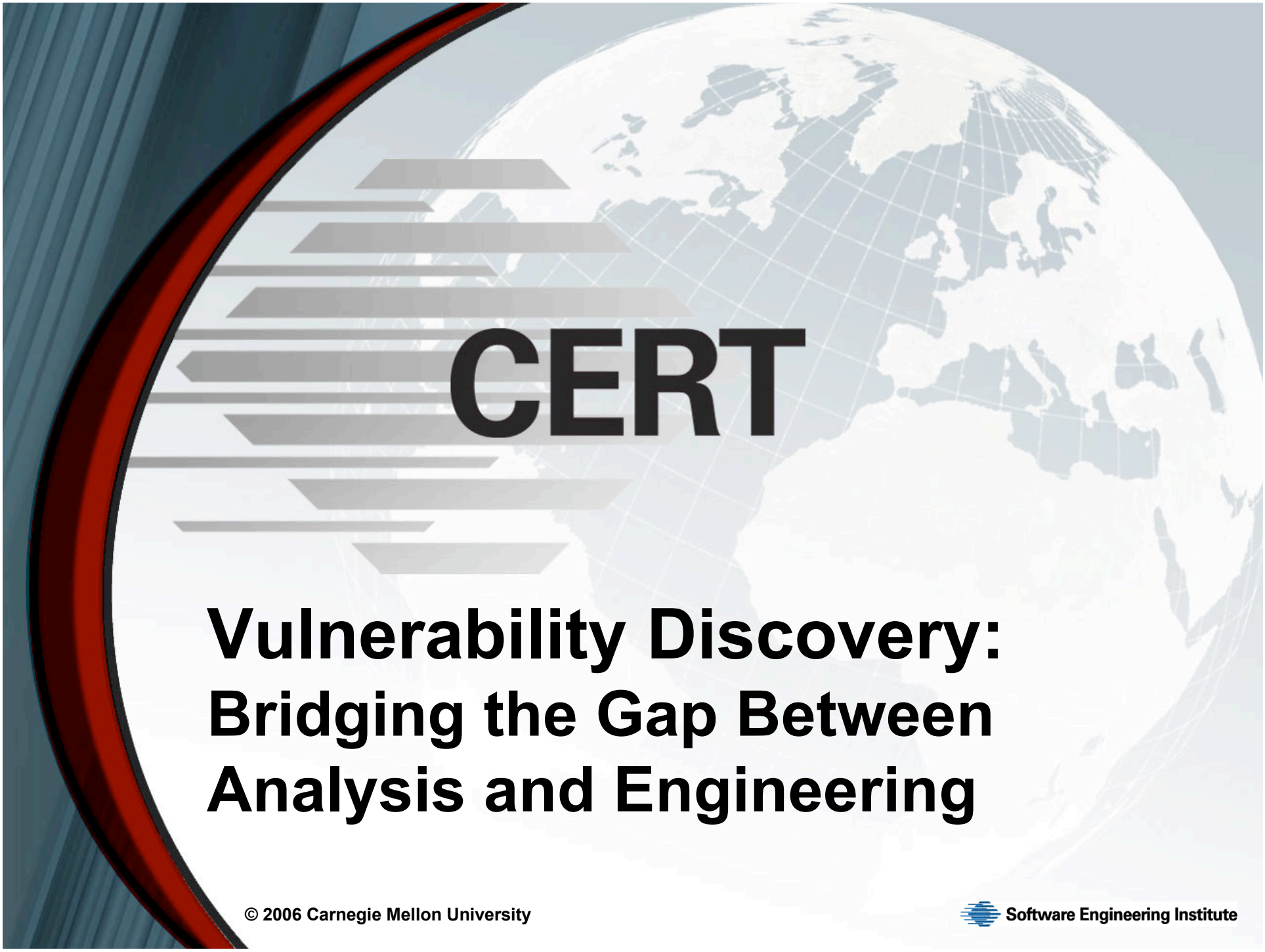


Vulnerability Discovery: Bridging the Gap Between Analysis and Engineering

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Vulnerability Discovery: Bridging the Gap Between Analysis and Engineering	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**22**	

Overture

Where are we today?

What is Vulnerability Discovery?

Problem Statement

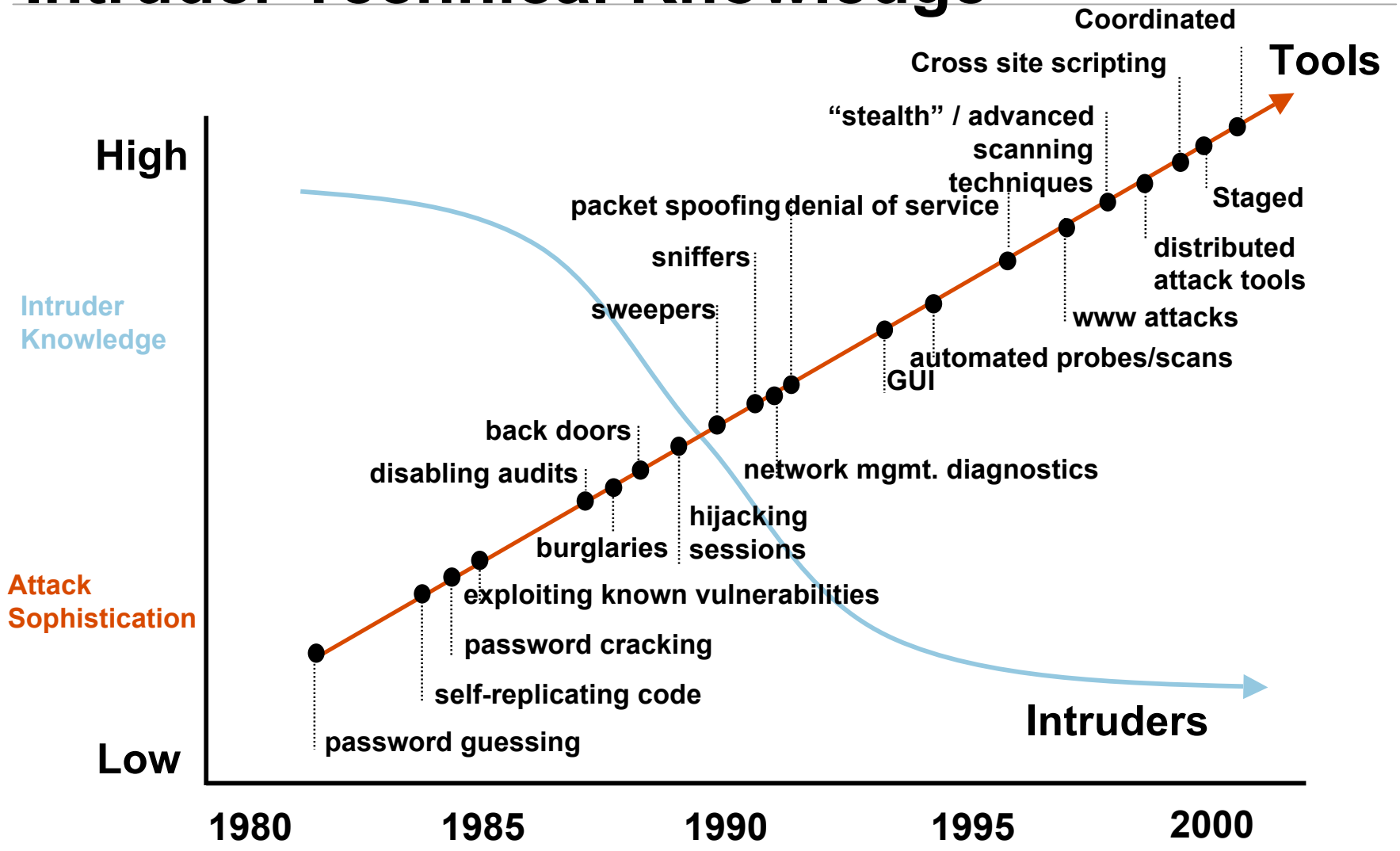
Why is this problem?

Who are we?

- Our Vision
- Our Agenda

Where are we today?

Attack Sophistication vs. Intruder Technical Knowledge



CERT

What is Vulnerability Discovery?

Vulnerability discovery is a process used to uncover and fix types of software defects with security impacts when present in information systems:

Vulnerabilities

Problem Statement (1)

Security analysts document:

- Preconditions for exploit
- Impacts of exploitation
- Remediation for system administrators

Gap: Underlying engineering causes

Problem Statement (2)

The vulnerability discovery process needs to reach a point where it can be ***systematically*** used by developers and testers to improve the practice of security engineering.

Problem Statement (3)

Today the discovery process is too ***ad-hoc*** for software engineers, who need:

- Root cause analysis (not just attack vectors)
- Line numbers of code, function points, data and execution path analysis, … .
- Tools, and the knowledge and motivation to use them in their process

Why is this a problem?

Because the security industry, by and large, is still too ***reactive***

And the later a vulnerability is found, the more costly it is to fix . . .

CERT

Who are we?

Vulnerability Researchers

CERT Coordination Center

Software Engineering Institute

Carnegie Mellon University

CERT

Our Vision

Enabling informed trust and confidence in a networked world means

Zero

vulnerabilities in software

CERT

Another Perspective

Finding vulnerabilities using test tools, techniques

Translating the context for properly fixing

Provide quality assurance as early in the product lifecycle, ideally *without exploits*

Goals

- Perform discovery work in a safe environment
- Transform analytical understanding into engineering knowledge
- Reduce the amount of time and effort (cost) required to find and fix vulnerabilities

WE DO THIS TODAY by BUILDING DISCOVERY TOOLS for ENGINEERS

Our Agenda

Translating our domain expertise into engineering knowledge and tools that can eliminate all known types of vulnerabilities as early in the product lifecycle as possible

CERT

Case Studies

Motivation:

To gain experience with knowledge, process, and tools useful as discovery agents

To understand potential engineering principles behind the discovery of software vulnerabilities

Results:

Targeted discovery work in selected technologies

An Easy Target: ActiveX

1995 – OLE 2 ➔ COM ➔ ActiveX

2000 – CERT/CC ActiveX Security Workshop

2005 – VU#680526 ➔ New vector for exploiting COM vulnerabilities via Internet Explorer discovered

2006 – Dranzer, the COM Object Tester

Other Applications

Red teaming and Penetration Testing

Targeted Critical Infrastructure Protection

Aid intelligence, law enforcement, and military operations

Vulnerability Re-Discovery

- To help reverse engineer attack tools
- To independently validate analysis
- To bridge the gap between discovers and analysts

Summary (1)

- Finding more effective test methods to discover vulnerabilities is hard and requires knowledge about vulnerabilities and the systems they are a part of

- Developing effective test tools requires knowledge, experimentation, innovation and time

Summary (2)

- Translating vulnerability analytical products into engineering knowledge is needed to bridge the current gap between the security community and the developer community

Questions

What questions do you folks have?

Coda

Vulnerability discovery is both a journey and a destination:

It needs a stable environment to thrive

It needs to become much more disciplined to create engineering knowledge

It needs a community of like-minded folks to grow tools and techniques

For More Information

Contact CERT/CC Vulnerability Discovery Project by email:

Subject: Vulnerability Discovery Project Request
To: cert@cert.org
Carbon Copy: jsh@cert.org

Visit the CERT® web site

URL: https://www.cert.org/

Contact CERT Coordination Center

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA

Hotline**: +1-412-268-7090**
CERT/CC personnel answer 24x7, 365.25 days per year

Fax: **+1-412-268-6989**

mailto:cert@cert.org